Cisco.300-715.vJan-2024.by.Erick.88q

Number: 300-715
Passing Score: 800
Time Limit: 120
File Version: 21.0

Exam Code: 300-715
Exam Name: Implementing and Configuring Cisco Identity Services Engine

Exam A

QUESTION 1
An engineer is implementing Cisco ISE and needs to configure 802.1X. The port settings are configured for port-based authentication. Which command should be used to complete this configuration?

A. dot1x pae authenticator
B. dot1x system-auth-control
C. authentication port-control auto
D. aaa authentication dot1x default group radius

Correct Answer: B
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/dot1x.html#wp1133395

QUESTION 2
Which two default endpoint identity groups does Cisco ISE create? (Choose two)

A. block list
B. endpoint
C. profiled
D. allow list
E. unknown

Correct Answer: C, E
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.htmlDefault Endpoint Identity Groups Created for EndpointsCisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints,Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such asCisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. Aparent group is the default identity group that exists in the system.
Cisco ISE creates the following endpoint identity groups:
Blacklist—This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are block listed in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.
GuestEndpoints—This endpoint identity group includes endpoints that are used by guest users.
Profiled—This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.
RegisteredDevices—This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and block these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blocked in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blocked devices to a URL, which displays "Unauthorised Network Access", a default portal page to the blocked devices.
Unknown—This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.
In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint identity groups, which are associated to the Profiled identity group:
Cisco-IP-Phone—An identity group that contains all the profiled Cisco IP phones on your network.
Workstation—An identity group that contains all the profiled workstations on your network.

QUESTION 3
In a standalone Cisco ISE deployment, which two personas are configured on a node? (Choose two)

A. publisher
B. administration
C. primary
D. policy service
E. subscriber

Correct Answer: B, D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010.html

QUESTION 4
What happens when an internal user is configured with an external identity store for authentication, but an engineer uses the Cisco ISE admin portal to select an internal identity store as the identity source?

A. Authentication is redirected to the internal identity source.
B. Authentication is redirected to the external identity source.
C. Authentication is granted.
D. Authentication fails.

Correct Answer: D
Section:

QUESTION 5
An engineer is configuring web authentication and needs to allow specific protocols to permit DNS traffic. Which type of access list should be used for this configuration?

A. reflexive ACL
B. extended ACL
C. standard ACL
D. numbered ACL

Correct Answer: B
Section:

QUESTION 6
Which two features should be used on Cisco ISE to enable the TACACS+ feature? (Choose two)

A. External TACACS Servers
B. Device Admin Service
C. Device Administration License
D. Server Sequence
E. Command Sets

Correct Answer: B, C
Section:

QUESTION 7
An employee logs on to the My Devices portal and marks a currently on-boarded device as 'Lost'.
Which two actions occur within Cisco ISE as a result oí this action? (Choose two)

A. Certificates provisioned to the device are not revoked
B. BYOD Registration status is updated to No
C. The device access has been denied
D. BYOD Registration status is updated to Unknown.
E. The device status is updated to Stolen

Correct Answer: A, B
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01111.html

QUESTION 8
An administrator connects an HP printer to a dot1x enable port, but the printer in not accessible Which feature must the administrator enable to access the printer?

A. MAC authentication bypass
B. change of authorization
C. TACACS authentication
D. RADIUS authentication

Correct Answer: A
Section:
Explanation:
https://community.cisco.com/t5/network-access-control/ise-for-printer-security/m-p/3933216

QUESTION 9
A new employee just connected their workstation to a Cisco IP phone. The network administrator wants to ensure that the Cisco IP phone remains online when the user disconnects their Workstation from the corporate network Which CoA configuration meets this requirement?

A. Port Bounce
B. Reauth
C. NoCoA
D. Disconnect

Correct Answer: C
Section:
Explanation:
https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-design

QUESTION 10
A network administrator must use Cisco ISE to check whether endpoints have the correct version of antivirus installed Which action must be taken to allow this capability?

A. Configure a native supplicant profile to be used for checking the antivirus version
B. Configure Cisco ISE to push the HostScan package to the endpoints to check for the antivirus version.
C. Create a Cisco AnyConnect Network Visibility Module configuration profile to send the antivirus information of the endpoints to Cisco ISE.

D. Create a Cisco AnyConnect configuration within Cisco ISE for the Compliance Module and associated configuration files

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_client_prov.htmlAbout Anyconnect Network Visibility Module
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect45/administration/guide/b_AnyConnect_Administrator_Guide_4-5/nvm.html

QUESTION 11
A network administrator must configura endpoints using an 802 1X authentication method with EAP identity certificates that are provided by the Cisco ISE When the endpoint presents the identity certificate to Cisco ISE to validate the certificate, endpoints must be authorized to connect to the network Which EAP type must be configured by the network administrator to complete this task?

A. EAP-PEAP-MSCHAPv2
B. EAP-TTLS
C. EAP-FAST
D. EAP-TLS

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/certificaterequirements-eap-tls-peapabout EAP FAST
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/eap-fast/200322-Understanding-EAP-FAST-and-Chaining-imp.html

QUESTION 12
Refer to the exhibit. An engineer is creating a new TACACS* command set and cannot use any show commands after togging into the device with this command set authorization Which configuration is causing this issue?

A. Question marks are not allowed as wildcards for command sets.
B. The command set is allowing all commands that are not in the command list
C. The wildcard command listed is in the wrong format
D. The command set is working like an ACL and denying every command.

Correct Answer: A
Section:

QUESTION 13
A network engineer must enforce access control using special tags, without re-engineering the network design. Which feature should be configured to achieve this in a scalable manner?

A. SGT
B. dACL
C. VLAN
D. RBAC

Correct Answer: A
Section:

QUESTION 14
What is the deployment mode when two Cisco ISE nodes are configured in an environment?

A. distributed
B. active
C. standalone
D. standard

Correct Answer: A
Section:

QUESTION 15
Which two roles are taken on by the administration person within a Cisco ISE distributed environment? (Choose two.)

A. backup
B. secondary
C. standby
D. primary
E. active

Correct Answer: B, D
Section:

QUESTION 16
A company is attempting to improve their BYOD policies and restrict access based on certain criteri a. The company's subnets are organized by building. Which attribute should be used in order to gain access based on location?

A. static group assignment
B. IP address
C. device registration status
D. MAC address

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html#ID1353

QUESTION 17
An engineer is migrating users from MAB to 802.1X on the network. This must be done during normal business hours with minimal impact to users. Which CoA method should be used?

A. Port Bounce
B. Port Shutdown
C. Session Termination
D. Session Reauthentication

Correct Answer: D
Section:

QUESTION 18
What occurs when a Cisco ISE distributed deployment has two nodes and the secondary node is deregistered?

A. The primary node restarts
B. The secondary node restarts.
C. The primary node becomes standalone
D. Both nodes restart.

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-1-1/installation_guide/ise_install_guide/ise_deploy.htmlif your deployment has two nodes and you deregister the secondary node, both nodes in thisprimary-secondary pair are restarted.
(The former primary and secondary nodes becomestandalone.)

QUESTION 19
Which port does Cisco ISE use for native supplicant provisioning of a Windows laptop?

A. TCP 8909
B. TCP 8905
C. UDP 1812
D. TCP 443

Correct Answer: B
Section:

QUESTION 20
Which statement about configuring certificates for BYOD is true?

A. An Android endpoint uses EST, whereas other operating systems use SCEP for enrollment
B. The SAN field is populated with the end user name.
C. An endpoint certificate is mandatory for the Cisco ISE BYOD
D. The CN field is populated with the endpoint host name

Correct Answer: C
Section:

QUESTION 21
What sends the redirect ACL that is configured in the authorization profile back to the Cisco WLC?

A. Cisco-av-pair
B. Class attribute
C. Event
D. State attribute

Correct Answer: A
Section:

QUESTION 22

Which two events trigger a CoA for an endpoint when CoA is enabled globally for ReAuth? (Choose two.)

A. endpoint marked as lost in My Devices Portal
B. addition of endpoint to My Devices Portal
C. endpoint profile transition from Apple-Device to Apple-iPhone
D. endpoint profile transition from Unknown to Windows 10-Workstation
E. updating of endpoint dACL.

Correct Answer: C, D
Section:

QUESTION 23
What is a requirement for Feed Service to work?

A. TCP port 3080 must be opened between Cisco ISE and the feed server
B. Cisco ISE has a base license.
C. Cisco ISE has access to an internal server to download feed update
D. Cisco ISE has Internet access to download feed update

Correct Answer: C
Section:

QUESTION 24
Which advanced option within a WLAN must be enabled to trigger Central Web Authentication for Wireless users on AireOS controller?

A. DHCP server
B. static IP tunneling
C. override Interface ACL
D. AAA override

Correct Answer: D
Section:

QUESTION 25
What is a valid guest portal type?

A. Sponsored-Guest
B. My Devices
C. Sponsor
D. Captive-Guest

Correct Answer: A
Section:

QUESTION 26
What is needed to configure wireless guest access on the network?

A. endpoint already profiled in ISE
B. WEBAUTH ACL for redirection
C. valid user account in Active Directory
D. Captive Portal Bypass turned on

Correct Answer: D
Section:

QUESTION 27
Which two methods should a sponsor select to create bulk guest accounts from the sponsor portal?
(Choose two)

A. Random
B. Monthly
C. Daily
D. Imported
E. Known

Correct Answer: A, D
Section:

QUESTION 28
How is policy services node redundancy achieved in a deployment?

A. by enabling VIP
B. by utilizing RADIUS server list on the NAD
C. by creating a node group
D. by deploying both primary and secondary node

Correct Answer: C
Section:

QUESTION 29
If a user reports a device lost or stolen, which portal should be used to prevent the device from accessing the network while still providing information about why the device is blocked?

A. Client Provisioning
B. Guest
C. BYOD
D. Blacklist

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.html#90273The Blacklist identity group is system generated and maintained by ISE to prevent access to lost orstolen devices. In this design guide, two authorization profiles are used to enforce the permissionsfor wireless and wired devices within the Blacklist:
Blackhole WiFi Access
Blackhole Wired Access

QUESTION 30

A user reports that the RADIUS accounting packets are not being seen on the Cisco ISE server.
Which command is the user missing in the switch's configuration?

A. radius-server vsa send accounting

B. aaa accounting network default start-stop group radius

C. aaa accounting resource default start-stop group radius

D. aaa accounting exec default start-stop group radios

Correct Answer: A
Section:

QUESTION 31

What are two benefits of TACACS+ versus RADIUS for device administration? (Choose two)

A. TACACS+ supports 802.1X, and RADIUS supports MAB

B. TACACS+ uses UDP, and RADIUS uses TCP

C. TACACS+ has command authorization, and RADIUS does not.

D. TACACS+ provides the service type, and RADIUS does not

E. TACACS+ encrypts the whole payload, and RADIUS encrypts only the password.

Correct Answer: C, E
Section:

QUESTION 32

Which two task types are included in the Cisco ISE common tasks support for TACACS+ profiles?
(Choose two.)

A. Firepower

B. WLC

C. IOS

D. ASA

E. Shell

Correct Answer: B, E
Section:
Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_0100010.htmlTACACS+ ProfileTACACS+ profiles control the initial login session of the device administrator. A session refers to eachindividual authentication, authorization, or accounting request. A session authorization request to anetwork device elicits an ISE response. The response includes a token that is interpreted by thenetwork device, which limits the commands that may be executed for the duration of a session. Theauthorization policy for a device administration access service can contain a single shell profile andmultiple command sets. The TACACS+ profile definitions are split into two components:

Common tasks

Custom attributes

There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles)—Task Attribute View and Raw View. Common tasks can be entered using the Task

Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.

The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft

specifications. However, the values can be used in the authorization of requests from other services.
In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:
Shell
WLC
Nexus
Generic
The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using a equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

QUESTION 33
What allows an endpoint to obtain a digital certificate from Cisco ISE during a BYOD flow?

A. Network Access Control
B. My Devices Portal
C. Application Visibility and Control
D. Supplicant Provisioning Wizard

Correct Answer: D
Section:

QUESTION 34
Which configuration is required in the Cisco ISE authentication policy to allow Central Web Authentication?

A. MAB and if user not found, continue
B. MAB and if authentication failed, continue
C. Dot1x and if user not found, continue
D. Dot1x and if authentication failed, continue

Correct Answer: A
Section:

QUESTION 35
Which portal is used to customize the settings for a user to log in and download the compliance module?

A. Client Profiling
B. Client Endpoint
C. Client Provisioning
D. Client Guest

Correct Answer: C
Section:

QUESTION 36
Which term refers to an endpoint agent that tries to join an 802 1X-enabled network?

A. EAP server
B. supplicant
C. client
D. authenticator

Correct Answer: B
Section:
Explanation:
https://www.oreilly.com/library/view/cisco-isefor/9780133103632/ch16.html#:~:text=What%20is%20a%20supplicant%3F,networks%2C%20both%20wired%20and%20wireless.&text=The%20802.1X%20transactions%20are,Identity%20Services%20Engine%20(ISE).

QUESTION 37
Which two features are available when the primary admin node is down and the secondary admin node has not been promoted? (Choose two.)

A. hotspot
B. new AD user 802 1X authentication
C. posture
D. BYOD
E. guest AUP

Correct Answer: B, C
Section:

QUESTION 38

Which protocol must be allowed for a BYOD device to access the BYOD portal?

A. HTTP
B. SMTP
C. HTTPS
D. SSH

Correct Answer: C
Section:

QUESTION 39
In which two ways can users and endpoints be classified for TrustSec?
(Choose Two.)

A. VLAN
B. SXP
C. dynamic
D. QoS
E. SGACL

Correct Answer: A, E
Section:

QUESTION 40
Which two features must be used on Cisco ISE to enable the TACACS. feature? (Choose two)

A. Device Administration License
B. Server Sequence
C. Command Sets
D. Enable Device Admin Service
E. External TACACS Servers

Correct Answer: A, D
Section:

QUESTION 41
During BYOD flow, from where does a Microsoft Windows PC download the Network Setup Assistant?

A. Cisco App Store
B. Microsoft App Store
C. Cisco ISE directly
D. Native OTA functionality

Correct Answer: C
Section:

QUESTION 42

Which use case validates a change of authorization?

A. An authenticated, wired EAP-capable endpoint is discovered
B. An endpoint profiling policy is changed for authorization policy.
C. An endpoint that is disconnected from the network is discovered
D. Endpoints are created through device registration for the guests

Correct Answer: B
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_prof_pol.html

QUESTION 43
A network engineer is configuring a network device that needs to filter traffic based on security group tags using a security policy on a routed into this task?

A. cts authorization list
B. cts role-based enforcement
C. cts cache enable
D. cts role-based policy priority-static

Correct Answer: B
Section:

QUESTION 44
An engineer is working with a distributed deployment of Cisco ISE and needs to configure various network probes to collect a set of attributes from the used to accomplish this task?

A. policy service
B. monitoring
C. pxGrid
D. primary policy administrator

Correct Answer: B
Section:

QUESTION 45

An engineer is configuring Cisco ISE to reprofile endpoints based only on new requests of INITREBOOT and SELECTING message types. Which probe should be used to accomplish this task?

A. MMAP
B. DNS
C. DHCP
D. RADIUS

Correct Answer: C
Section:

QUESTION 46
An engineer is using Cisco ISE and configuring guest services to allow wireless devices to access the network. Which action should accomplish this task?

A. Create the redirect ACL on the WLC and add it to the WLC policy
B. Create the redirect ACL on the WLC and add it to the Cisco ISE policy.
C. Create the redirect ACL on Cisco ISE and add it to the WLC policy
D. Create the redirect ACL on Cisco ISE and add it to the Cisco ISE Policy

Correct Answer: B
Section:

QUESTION 47
An engineer is configuring web authentication using non-standard ports and needs the switch to redirect traffic to the correct port. Which command should be used to accomplish this task?

A. permit tcp any any eq <port number>
B. aaa group server radius proxy
C. ip http port <port number>
D. aaa group server radius

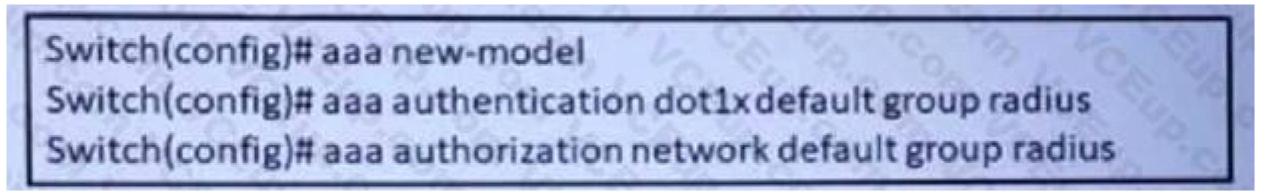
Correct Answer: C
Section:

QUESTION 48
An administrator needs to connect ISE to Active Directory as an external authentication source and allow the proper ports through the firewall. Which two ports should be opened to accomplish this task? (Choose two)

A. TELNET 23
B. LDAP 389
C. HTTP 80
D. HTTPS 443
E. MSRPC 445

Correct Answer: B, E
Section:

QUESTION 49
Refer to the exhibit.



```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius
```

A network engineers configuring the switch to accept downloadable ACLs from a Cisco ISC server Which two commands should be run to complete the configuration? (Choose two)

A. aaa authorization auth-proxy default group radius
B. radius server vsa sand authentication
C. radius-server attribute 8 include-in-access-req
D. ip device tracking
E. dot1x system-auth-control

Correct Answer: B, C
Section:

QUESTION 50
An engineer is using the low-impact mode for a phased deployment of Cisco ISE and is trying to connect to the network prior to authentication. Which access will be denied in this?

A. HTTP
B. DNS
C. EAP
D. DHCP

Correct Answer: A
Section:

QUESTION 51
A network engineer needs to ensure that the access credentials are not exposed during the 802.1x authentication among components. Which two protocols should complete this task?

A. PEAP
B. EAP-MD5
C. LEAP
D. EAP-TLS
E. EAP-TTLS

Correct Answer: B, D
Section:

QUESTION 52
An engineer is configuring a guest password policy and needs to ensure that the password complexity requirements are set to mitigate brute force attacks. Which two requirement complete this policy? (Choose two)

A. minimum password length
B. active username limit
C. access code control
D. gpassword expiration period
E. username expiration date

Correct Answer: A, D
Section:

QUESTION 53
Which two actions occur when a Cisco ISE server device administrator logs in to a device? (Choose two)

A. The device queries the internal identity store
B. The Cisco ISE server queries the internal identity store
C. The device queries the external identity store
D. The Cisco ISE server queries the external identity store.
E. The device queries the Cisco ISE authorization server

Correct Answer: A, D
Section:

QUESTION 54
When planning for the deployment of Cisco ISE, an organization's security policy dictates that they must use network access authentication via RADIUS. It also states that the deployment provide an adequate amount of security and visibility for the hosts on the network. Why should the engineer configure MAB in this situation?

A. The Cisco switches only support MAB.
B. MAB provides the strongest form of authentication available.
C. The devices in the network do not have a supplicant.
D. MAB provides user authentication.

Correct Answer: C
Section:

QUESTION 55
In a Cisco ISE split deployment model, which load is split between the nodes?

A. AAA
B. network admission
C. log collection
D. device admission

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/install_guide/b_ise_InstallationGuide26.pdf

QUESTION 56
What must be configured on the WLC to configure Central Web Authentication using Cisco ISE and a WLC?

A. Set the NAC State option to SNMP NAC.
B. Set the NAC State option to RADIUS NAC.
C. Use the radius-server vsa send authentication command.
D. Use the ip access-group webauth in command.

Correct Answer: B
Section:

QUESTION 57

Refer to the exhibit.

An organization recently implemented network device administration using Cisco ISE. Upon testing the ability to access all of the required devices, a user in the Cisco ISE group IT Admins is attempting to login to a device in their organization's finance department but is unable to. What is the problem?

A. The IT training rule is taking precedence over the IT Admins rule.

B. The authorization conditions wrongly allow IT Admins group no access to finance devices.

C. The finance location is not a condition in the policy set.

D. The authorization policy doesn't correctly grant them access to the finance devices.

Correct Answer: D
Section:

QUESTION 58

When creating a policy within Cisco ISE for network access control, the administrator wants to allow different access restrictions based upon the wireless SSID to which the device is connecting. Which policy condition must be used in order to accomplish this?

A. Network Access NetworkDeviceName CONTAINS <SSID Name>

B. DEVICE Device Type CONTAINS <SSID Name>

C. Radius Called-Station-ID CONTAINS <SSID Name>

D. Airespace Airespace-Wlan-ld CONTAINS <SSID Name>

Correct Answer: C

Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115734-ise-policiesssid-00.html

QUESTION 59
There is a need within an organization for a new policy to be created in Cisco ISE. It must validate that a specific anti-virus application is not only installed, but running on a machine before it is allowed access to the network. Which posture condition should the administrator configure in order for this policy to work?

A. file
B. registry
C. application
D. service

Correct Answer: C
Section:

QUESTION 60
An organization wants to improve their BYOD processes to have Cisco ISE issue certificates to the BYOD endpoints. Currently, they have an active certificate authority and do not want to replace it with Cisco ISE. What must be configured within Cisco ISE to accomplish this goal?

A. Create a certificate signing request and have the root certificate authority sign it.
B. Add the root certificate authority to the trust store and enable it for authentication.
C. Create an SCEP profile to link Cisco ISE with the root certificate authority.
D. Add an OCSP profile and configure the root certificate authority as secondary.

Correct Answer: C
Section:
Explanation:
Ref:https://www.cisco.com/c/en/us/support/docs/security/identity-services-enginesoftware/116068-configure-product-00.html

QUESTION 61
An administrator is adding network devices for a new medical building into Cisco ISE. These devices must be in a network device group that is identifying them as "Medical Switch" so that the policies can be made separately for the endpoints connecting through them. Which configuration item must be changed in the network device within Cisco ISE to accomplish this goal?

A. Change the device type to Medical Switch.
B. Change the device profile to Medical Switch.
C. Change the model name to Medical Switch.
D. Change the device location to Medical Switch.

Correct Answer: A
Section:

QUESTION 62
An engineer is designing a new distributed deployment for Cisco ISE in the network and is considering failover options for the admin nodes. There is a need to ensure that an admin node is available for configuration of policies at all times.
What is the requirement to enable this feature?

A. one primary admin and one secondary admin node in the deployment

B. one policy services node and one secondary admin node
C. one policy services node and one monitoring and troubleshooting node
D. one primary admin node and one monitoring and troubleshooting node

Correct Answer: A
Section:

QUESTION 63
A company manager is hosting a conference. Conference participants must connect to an open guest SSID and only use a preassigned code that they enter into the guest portal prior to gaining access to the network. How should the manager configure Cisco ISE to accomplish this goal?

A. Create entries in the guest identity group for all participants.
B. Create an access code to be entered in the AUP page.
C. Create logins for each participant to give them sponsored access.
D. Create a registration code to be entered on the portal splash page.

Correct Answer: B
Section:

QUESTION 64
A network security engineer needs to configure 802.1X port authentication to allow a single host to be authenticated for data and another single host to be authenticated for voice. Which command should the engineer run on the interface to accomplish this goal?

A. authentication host-mode single-host
B. authentication host-mode multi-auth
C. authentication host-mode multi-host
D. authentication host-mode multi-domain

Correct Answer: D
Section:

QUESTION 65
When setting up profiling in an environment using Cisco ISE for network access control, an organization must use non-proprietary protocols for collecting the information at layer 2. Which two probes will provide this information without forwarding SPAN packets to Cisco ISE? {Choose two.)

A. DHCP SPAN probe
B. SNMP query probe
C. NetFlow probe
D. RADIUS probe
E. DNS probe

Correct Answer: B, D
Section:
Explanation:
https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-design

QUESTION 66
What is a function of client provisioning?

A. Client provisioning ensures that endpoints receive the appropriate posture agents.
B. Client provisioning checks a dictionary attribute with a value.
C. Client provisioning ensures an application process is running on the endpoint.
D. Client provisioning checks the existence, date, and versions of the file on a client.

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_client_prov.html#:~:text=After%20Cisco%20ISE%20classifies%20a,packages%20and%20profiles%2C%20if%20necessary.

QUESTION 67
An engineer is testing Cisco ISE policies in a lab environment with no support for a deployment server. In order to push supplicant profiles to the workstations for testing, firewall ports will need to be opened. From which Cisco ISE persona should this traffic be originating?

A. monitoring
B. policy service
C. administration
D. authentication

Correct Answer: B
Section:

QUESTION 68
What is an advantage of using EAP-TLS over EAP-MS-CHAPv2 for client authentication?

A. EAP-TLS uses a username and password for authentication to enhance security, while EAP-MSCHAPv2 does not.
B. EAP-TLS secures the exchange of credentials, while EAP-MS-CHAPv2 does not.
C. EAP-TLS uses a device certificate for authentication to enhance security, while EAP-MS-CHAPv2 does not.
D. EAP-TLS uses multiple forms of authentication, while EAP-MS-CHAPv2 only uses one.

Correct Answer: C
Section:

QUESTION 69
There are several devices on a network that are considered critical and need to be placed into the ISE database and a policy used for them. The organization does not want to use profiling. What must be done to accomplish this goal?

A. Enter the MAC address in the correct Endpoint Identity Group.
B. Enter the MAC address in the correct Logical Profile.
C. Enter the IP address in the correct Logical Profile.
D. Enter the IP address in the correct Endpoint Identity Group.

Correct Answer: A
Section:

QUESTION 70

An engineer is tasked with placing a guest access anchor controller in the DMZ. Which two ports or port sets must be opened up on the firewall to accomplish this task? (Choose two.)

A. UDP port 1812 RADIUS
B. TCP port 161
C. TCP port 514
D. UDP port 79
E. UDP port 16666

Correct Answer: B, C
Section:

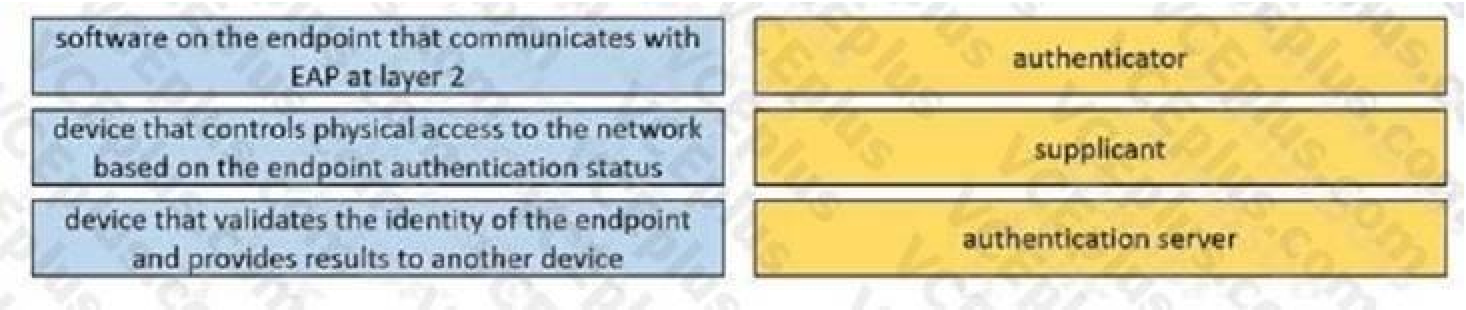
QUESTION 71
A network administrator is configuring authorization policies on Cisco ISE There is a requirement to use AD group assignments to control access to network resources After a recent power failure and Cisco ISE rebooting itself, the AD group assignments no longer work What is the cause of this issue?

A. The AD join point is no longer connected.
B. The AD DNS response is slow.
C. The certificate checks are not being conducted.
D. The network devices ports are shut down.

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/ise_active_directory_integration/b_ISE_AD_integration_2x.html#ID612

QUESTION 72
DRAG DROP
Drag the descriptions on the left onto the components of 802.1X on the right.

Select and Place:



software on the endpoint that communicates with EAP at layer 2

device that controls physical access to the network based on the endpoint authentication status

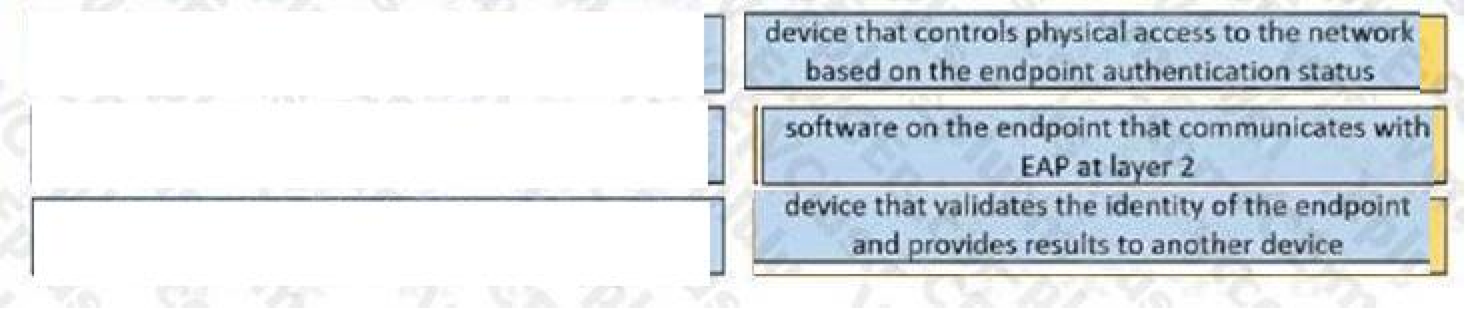
device that validates the identity of the endpoint and provides results to another device

authenticator

supplicant

authentication server

Correct Answer:



device that controls physical access to the network based on the endpoint authentication status

software on the endpoint that communicates with EAP at layer 2

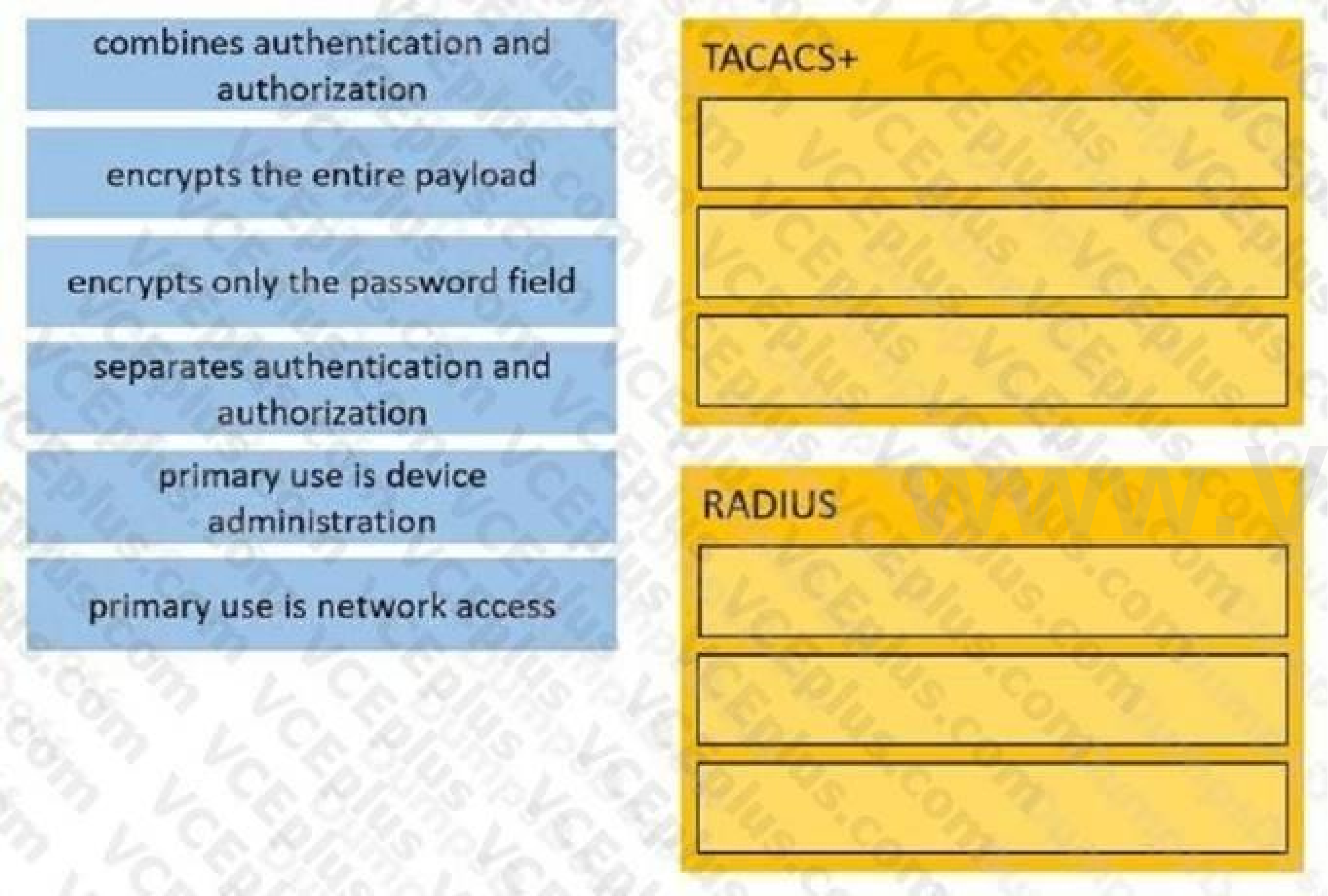
device that validates the identity of the endpoint and provides results to another device

Section:

Explanation:
Authenticator – device that controls physical access to the network based on the authentication status
Supplicant - software on the endpoint that communicates with EAP at layer 2
Authentication server – device that validates the identity of the endpoint and provides results to another device
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

QUESTION 73
DRAG DROP
Drag and drop the description from the left onto the protocol on the right that is used to carry out system authentication, authorization, and accounting.

Select and Place:



combines authentication and authorization

encrypts the entire payload

encrypts only the password field

separates authentication and authorization

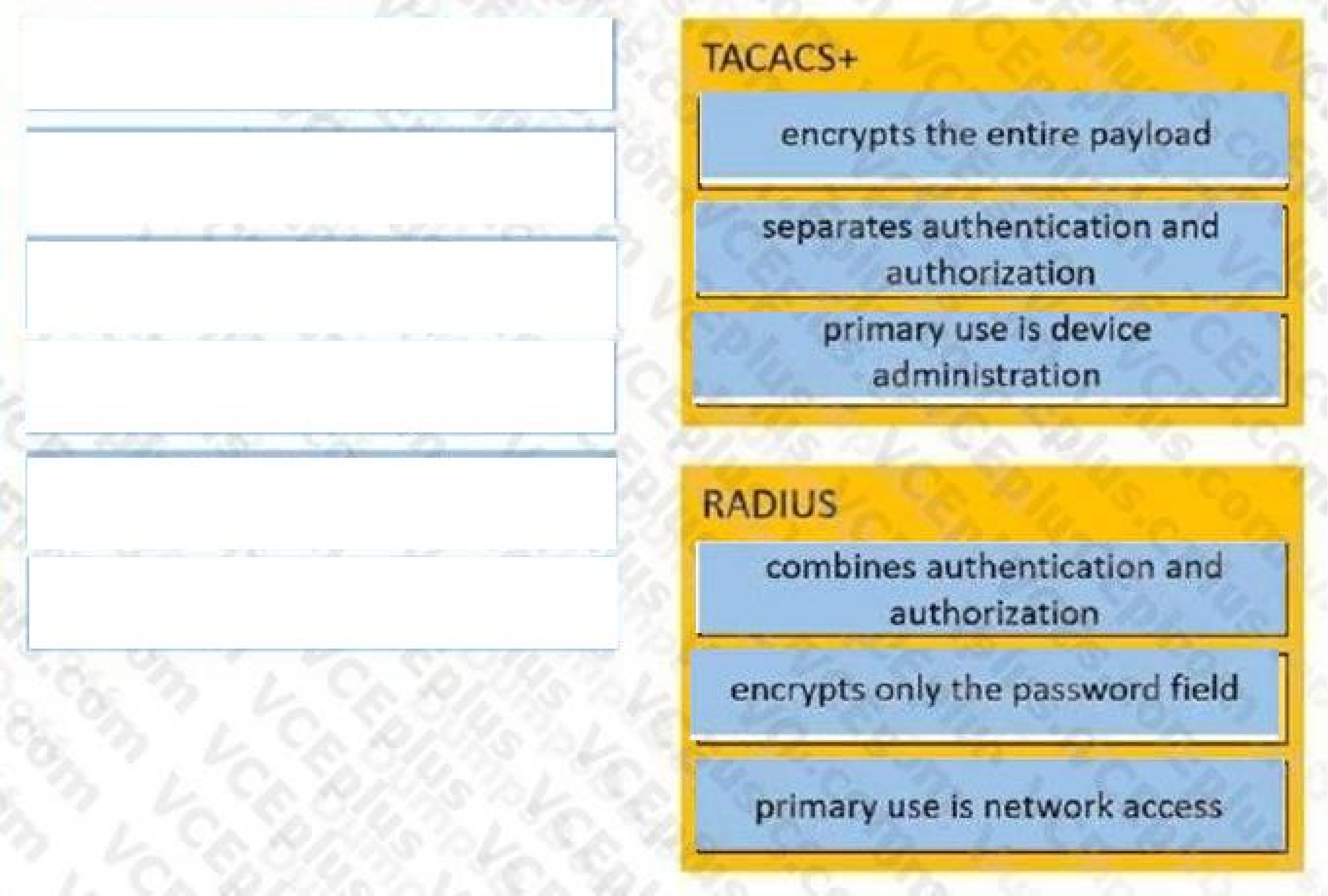
primary use is device administration

primary use is network access

TACACS+

RADIUS

Correct Answer:



TACACS+

encrypts the entire payload

separates authentication and authorization

primary use is device administration

RADIUS

combines authentication and authorization

encrypts only the password field

primary use is network access

Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-userservice-radius/13838-10.html

QUESTION 74
An engineer is configuring the remote access VPN to use Cisco ISE for AAA and needs to conduct posture checks on the connecting endpoints After the endpoint connects, it receives its initial authorization result and continues onto the compliance scan What must be done for this AAA configuration to allow compliant access to the network?

A. Configure the posture authorization so it defaults to unknown status
B. Fix the CoA port number
C. Ensure that authorization only mode is not enabled
D. Enable dynamic authorization within the AAA server group

Correct Answer: D
Section:

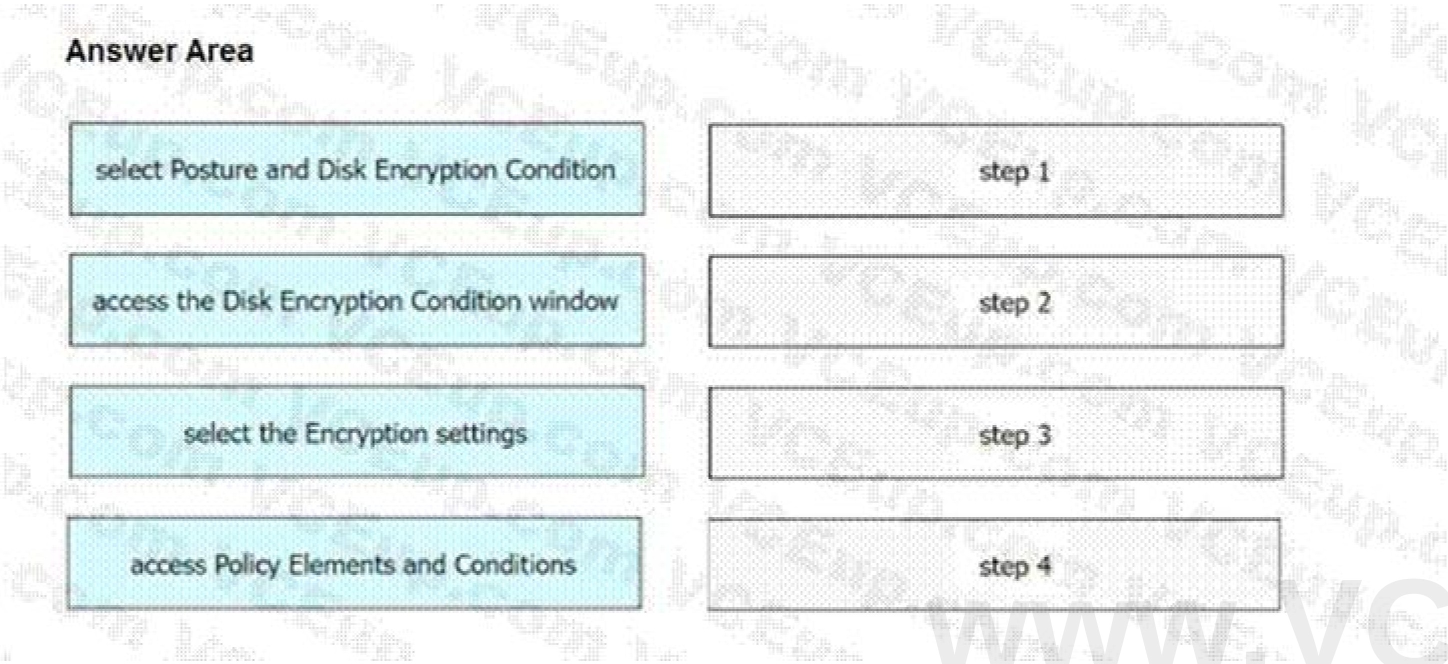
QUESTION 75
Which two Cisco ISE deployment models require two nodes configured with dedicated PAN and MnT personas? (Choose two.)

A. three PSN nodes
B. seven PSN nodes with one PxGrid node
C. five PSN nodes with one PxGrid node
D. two PSN nodes with one PxGrid node
E. six PSN nodes

Correct Answer: C, D
Section:

QUESTION 76
DRAG DROP
An engineer needs to configure a compliance policy on Cisco ISE to ensure that the latest encryption software is running on the C drive of all endpoints. Drag and drop the configuration steps from the left into the sequence on the right to accomplish this task.

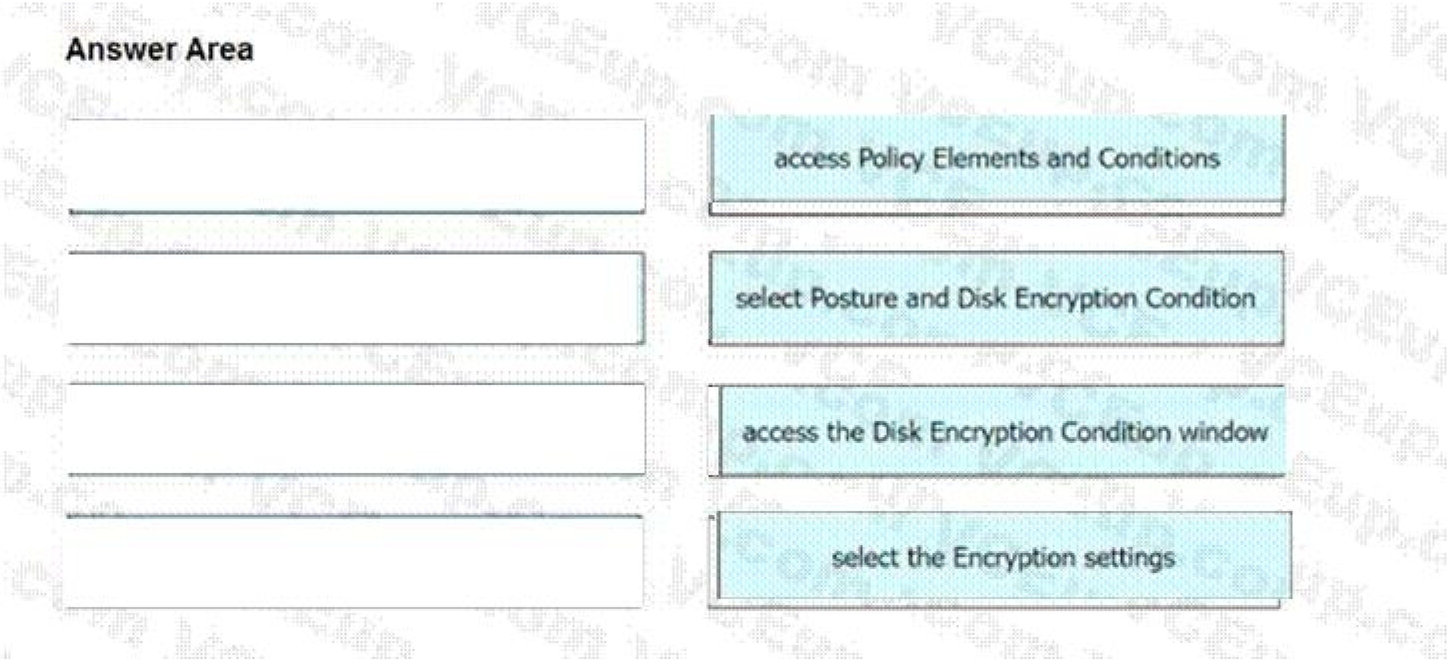
Select and Place:



Answer Area

select Posture and Disk Encryption Condition	step 1
access the Disk Encryption Condition window	step 2
select the Encryption settings	step 3
access Policy Elements and Conditions	step 4

Correct Answer:



Answer Area

	access Policy Elements and Conditions
	select Posture and Disk Encryption Condition
	access the Disk Encryption Condition window
	select the Encryption settings

Section:
Explanation:

QUESTION 77
An administrator is adding a switch to a network that is running Cisco ISE and is only for IP Phones The phones do not have the ability to authenticate via 802 1X Which command is needed on each switch port for

authentication?

A. dot1x system-auth-control
B. enable bypass-mac
C. enable network-authentication
D. mab

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-2mt/sec-configmab.html

QUESTION 78
A network administrator is setting up wireless guest access and has been unsuccessful in testing client access. The endpoint is able to connect to the SSID but is unable to grant access to the guest network through the guest portal. What must be done to identify the problem?

A. Use context visibility to verify posture status.
B. Use the endpoint ID to execute a session trace.
C. Use the identity group to validate the authorization rules.
D. Use traceroute to ensure connectivity.

Correct Answer: B
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_011001.html#concept_87916A77E8774545B36D0BB422429596

QUESTION 79
A network administrator is configuring a secondary cisco ISE node from the backup configuration of the primary cisco ISE node to create a high availability pair The Cisco ISE CA certificates and keys must be manually backed up from the primary Cisco ISE and copied into the secondary Cisco ISE Which command most be issued for this to work?

A. copy certificate Ise
B. application configure Ise
C. certificate configure Ise
D. Import certificate Ise

Correct Answer: B
Section:
Explanation:
https://community.cisco.com/t5/network-access-control/ise-certificate-import-export/m-p/3847746

QUESTION 80
An organization is migrating its current guest network to Cisco ISE and has 1000 guest users in the current database There are no resources to enter this information into the Cisco ISE database manually. What must be done to accomplish this task effciently?

A. Use a CSV file to import the guest accounts
B. Use SOL to link me existing database to Ctsco ISE
C. Use a JSON fie to automate the migration of guest accounts
D. Use an XML file to change the existing format to match that of Cisco ISE

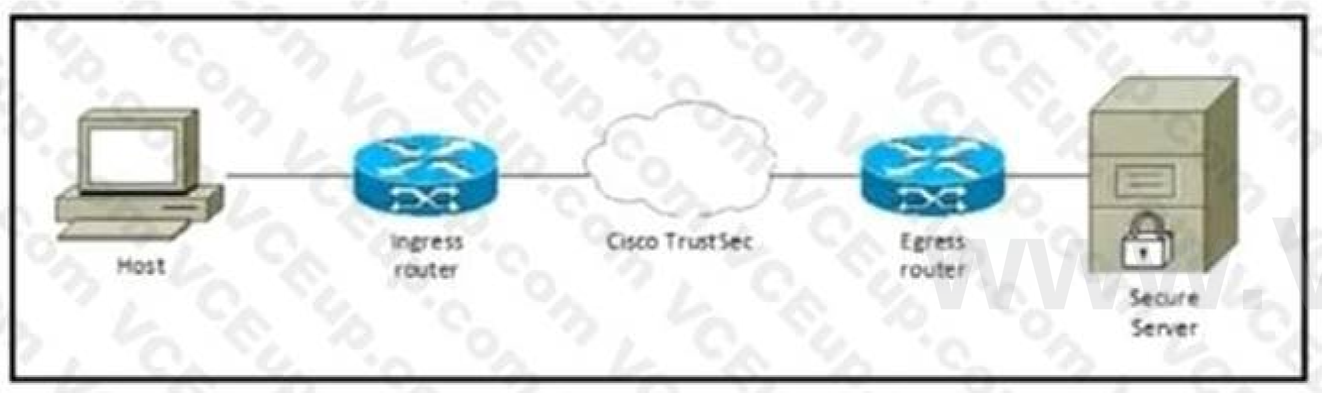
Correct Answer: A
Section:

QUESTION 81
MacOS users are complaining about having to read through wordy instructions when remediating their workstations to gam access to the network Which alternate method should be used to tell users how to remediate?

A. URL link
B. message text
C. executable
D. file distribution

Correct Answer: A
Section:
Explanation:
https://www.sciencedirect.com/topics/computer-science/remediation-action

QUESTION 82
Refer to the exhibit:



Refer to the exhibit Which component must be configured to apply the SGACL?

A. egress router
B. host
C. secure server
D. ingress router

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html#52796

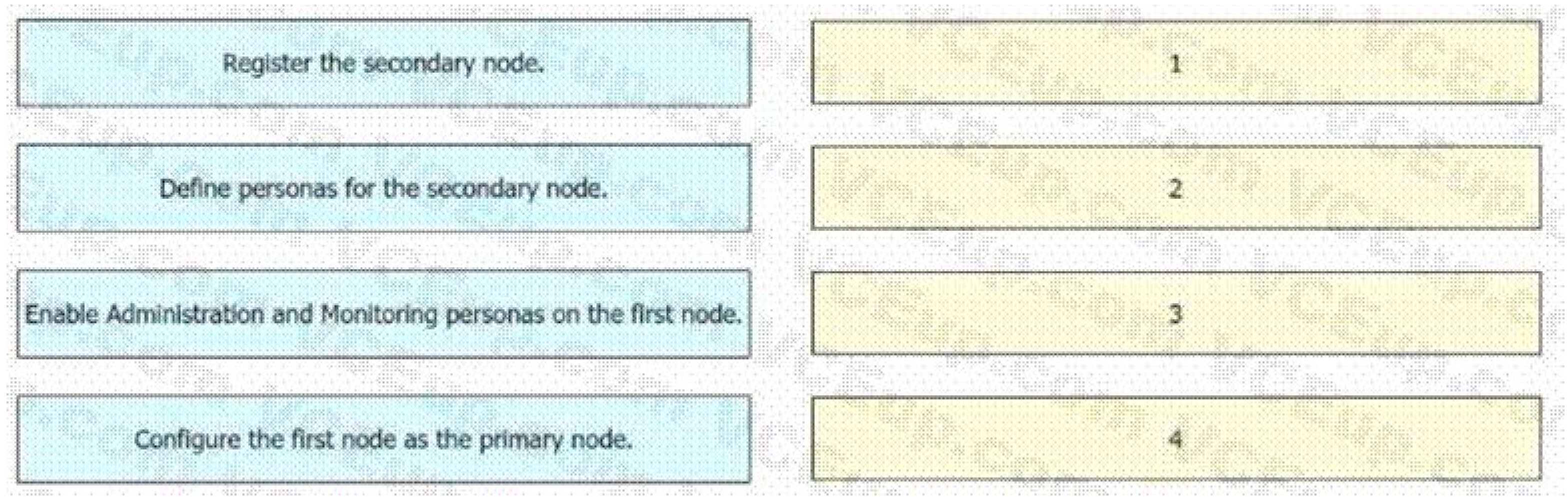
QUESTION 83
What does a fully distributed Cisco ISE deployment include?

A. PAN and PSN on the same node while MnTs are on their own dedicated nodes.
B. PAN and MnT on the same node while PSNs are on their own dedicated nodes.
C. All Cisco ISE personas on their own dedicated nodes.
D. All Cisco ISE personas are sharing the same node.

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_setup_cisco_ise.html

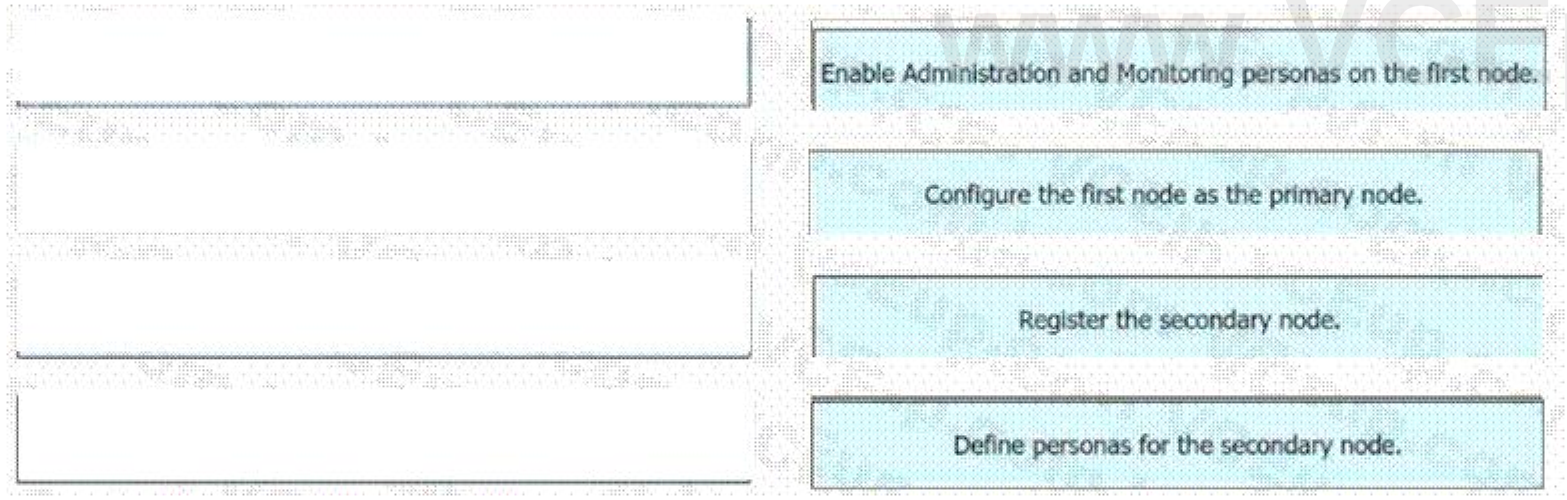
QUESTION 84
DRAG DROP
Drag and drop the configuration steps from the left into the sequence on the right to install two Cisco ISE nodes in a distributed deployment.

Select and Place:



Register the secondary node.	1
Define personas for the secondary node.	2
Enable Administration and Monitoring personas on the first node.	3
Configure the first node as the primary node.	4

Correct Answer:



Enable Administration and Monitoring personas on the first node.

Configure the first node as the primary node.

Register the secondary node.

Define personas for the secondary node.

Section:
Explanation:

QUESTION 85
Which Cisco ISE deployment model is recommended for an enterprise that has over 50,000 concurrent active endpoints?

A. large deployment with fully distributed nodes running all personas
B. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with shared PSNs
C. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with dedicated PSNs
D. small deployment with one primary and one secondary node running all personas

Correct Answer: C

Section:

QUESTION 86
What is a restriction of a standalone Cisco ISE node deployment?

A. Only the Policy Service persona can be disabled on the node.
B. The domain name of the node cannot be changed after installation.
C. Personas are enabled by default and cannot be edited on the node.
D. The hostname of the node cannot be changed after installation.

Correct Answer: C
Section:

QUESTION 87
An administrator is configuring cisco ISE lo authenticate users logging into network devices using TACACS+ The administrator is not seeing any o the authentication in the TACACS+ live logs. Which action ensures the users are able to log into the network devices?

A. Enable the device administration service in the Administration persona
B. Enable the session services in the administration persona
C. Enable the service sessions in the PSN persona.
D. Enable the device administration service in the PSN persona.

Correct Answer: D
Section:
Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_tacacs_device_admin.html

QUESTION 88
An engineer is working on a switch and must tag packets with SGT values such that it learns via SXP. Which command must be entered to meet this requirement?

A. ip source guard
B. ip dhcp snooping
C. ip device tracking maximum
D. ip arp inspection

Correct Answer: C
Section:
Explanation:
The ip device tracking maximum command is used to configure the maximum number of IP-to-SGT bindings that can be learned via SXP on a switch1. This command also enables the switch to tag packets with SGT values based on the bindings learned from SXP peers. The other commands are not related to SGT tagging or SXP learning.